

PARTIAL TRANSLATION OF JP 10(1998)-69463 A

Publication Date: March 10, 1998

Title of the Invention: PERSONAL IDENTIFICATION CONFIRMATION SYSTEM

Patent Application Number: 8-226986

Filing Date: August 28, 1996

Inventor: Katsuhiko OKADA

Applicants: Katsuhiko OKADA and Hideji IWAMOTO

(Page 5, right column, line 46 – Page 6, left column, line 27)

[0037] A retina pattern reading machine 10 of B bank can conduct collation with an already registered pattern, as well as registration. In this machine, when a user presses a collation key 13 while peeping through a finder 11 with one eye, the already registered corresponding pattern is extracted, and an identifier (IDA, etc.) of the registered person and a collation ratio can be displayed on a front display 15.

[0038] A collation ratio varies for each collation due to the angle of a peeping eye, a posture, and the like. In the case where a collation ratio with the already registered closest pattern is a predetermined reference value (e.g., 70%) or more, a retina pattern is determined to be identical with the registered one, and an identifier of the closest pattern is displayed together with a collation ratio. In the case where a collation ratio of a reference value or more cannot be obtained, a comment showing the case where there is no corresponding registered retina is displayed on the front display 15.

[0039] At affiliate shop R, a retina pattern reading machine 20 of handy reader 200 type is disposed. A salesclerk requests a user to declare that he/she is qualified by allowing a card CD represented by the user to be read by a card reader CR, and allows the user to peep through a finder 21 and press a collation switch 22. Because of this, at a confirmation company H,

an input retina pattern is collated with an already registered pattern by collation means 2 consisting of software resource cooperating with the retina pattern reading machine 20, the closest pattern with a collation ratio of a reference value (70%) or more is selected, and an identifier (IDB, etc.) corresponding to this pattern is extracted.

[0040] A reference value of a collation ratio is determined depending upon to which degree an error ratio is allowed. In the case of a reference value of 70%, an error ratio becomes about once per several 100,000 to 1,000,000 cases, which has no practical problem. A value higher or lower than this value may be selected.

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10069463 A

(43) Date of publication of application: 10.03.98

(51) Int. Cl

**G06F 15/00**  
**A61B 5/117**  
**G07F 7/08**

(21) Application number: 08226986

(22) Date of filing: 28.08.96

(71) Applicant: OKADA KATSUHIKO IWAMOTO  
HIDEJI

(72) Inventor: OKADA KATSUHIKO

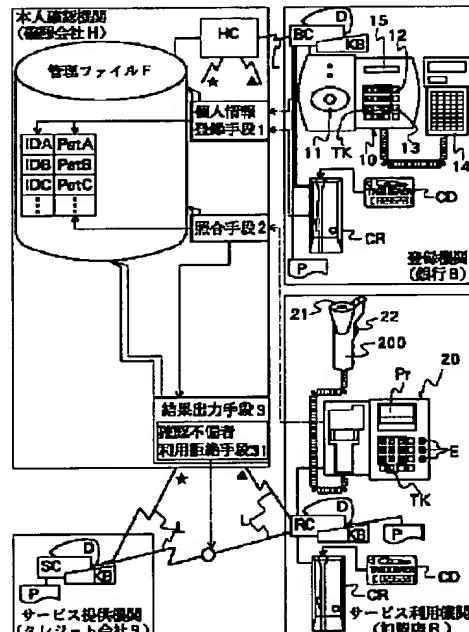
**(54) PERSONAL IDENTIFICATION CONFIRMATION SYSTEM**

**(57) Abstract:**

**PROBLEM TO BE SOLVED:** To confirm a qualified person himself truly capable of utilizing a credit under high security and to cut the illegal utilization by a third person.

**SOLUTION:** The retina patterns PatA, PatB... of respective credit members A, B... are registered in the file F of a management company H along with identifiers IDA, IDB... recorded on a card CD. At the utilization of the credit, a user makes the retina pattern be read from a reader 20 at a member shop R and receives collation with a registered pattern. When the inputted pattern matches with the already registered pattern corresponding to the identifier read from the card CD, personal identification is confirmed and the credit is not admitted as illegal utilization in the other case.

COPYRIGHT: (C)1998,JPO



## (12) 公開特許公報(A)

特開平10-69463

(43) 公開日 平成10年(1998)3月10日

(51) Int. C1. <sup>6</sup>	識別記号	府内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 F
A 6 1 B 5/117		0277-2 J	A 6 1 B 5/10	3 2 0 Z
G 0 7 F 7/08			G 0 7 F 7/08	Z

審査請求 未請求 請求項の数 11 O L (全 11 頁)

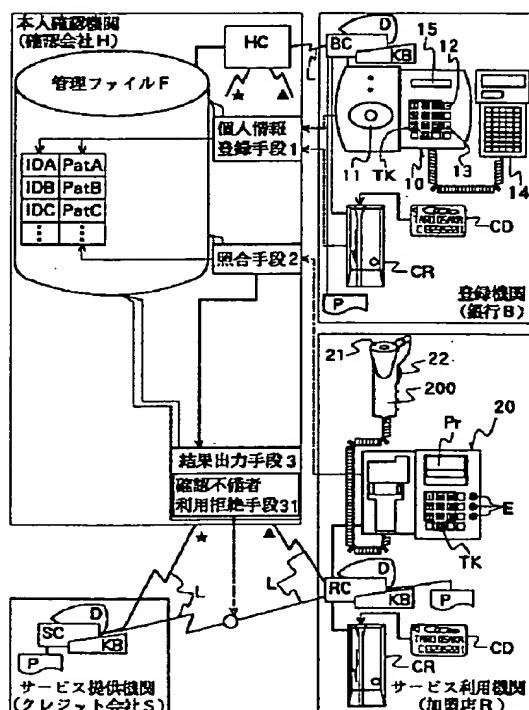
(21) 出願番号	特願平8-226986	(71) 出願人	595097793 岡田 勝彦 大阪府堺市東八田263番地の3
(22) 出願日	平成8年(1996)8月28日	(71) 出願人	596042682 岩本 秀治 大阪府八尾市高安町南1丁目20番地
		(72) 発明者	岡田 勝彦 大阪府堺市東八田263-3
		(74) 代理人	弁理士 廣瀬 邦夫

## (54) 【発明の名称】本人確認システム

## (57) 【要約】

【課題】 高いセキュリティの下で、真にクレジットを利用し得る資格者本人たることを確認し、第三者の不正利用をカットする。

【解決手段】 各クレジット会員 A, B … の網膜パターン P a t A, P a t B … を、カード C D に記録された識別子 I D A, I D B … と共に管理会社 H のファイル F に登録しておく。クレジットの利用時、利用者は加盟店 R で網膜パターンを読み取り機 2 0 から読み込まれ、登録パターンとの照合を受ける。この入力したパターンがカード C D から読み取る識別子に対応した既登録パターンと一致すれば、本人たることを確認し、それ以外の場合は、不正利用としてクレジットを認めない。



1

## 【特許請求の範囲】

【請求項1】 資格者本人にサービスを提供する提供側とこのサービスを利用する利用側との間に介在して、サービス利用者が資格者本人であるか否かを確認する本人確認システムであって、人の身体的個人情報を識別子と共に管理ファイル上に登録する個人情報登録手段

(1)、資格者たることを申告してサービスを利用する者が入力する身体的個人情報と既登録個人情報を照合する照合手段(2)、入力した利用者の身体的個人情報と申告にかかる資格者の既登録個人情報が一致して資格者本人を確認する場合とこれ以外の場合とを峻別する峻別出力を発する結果出力手段(3)を備えていることを特徴とする本人確認システム。

【請求項2】 結果出力手段(3)は、資格者本人を確認できない場合、サービスの利用拒絶出力を発する確認不備者利用拒絶手段(31)である請求項1記載の本人確認システム。

【請求項3】 識別子は、資格者たることを申告するサービス利用時に認識可能な情報であり、結果出力手段(3)は、入力した利用者の身体的個人情報と一致する既登録個人情報に付された識別子をサービスの利用側に通知する識別子通知手段(32)である請求項1記載の本人確認システム。

【請求項4】 サービスの利用時に身体的個人情報と併用して入力する識別子により、照合する既登録個人情報を検索する検索手段(4)を備えている請求項1～3何れか一記載の本人確認システム。

【請求項5】 サービスの利用時に身体的個人情報と併用して入力する識別子により、照合する既登録個人情報を検索する検索手段(4)、検索した既登録個人情報と入力した個人情報とが不一致の場合、入力した個人情報と他の既登録個人情報を照合するリカバリー手段(40)を備えている請求項3記載の本人確認システム。

【請求項6】 識別子は、サービスの利用資格証であるカードに記録されたカード情報から成る請求項1～5何れか一記載の本人確認システム。

【請求項7】 身体的個人情報の登録者に対応するプライベートデータにアクセスするデータアクセス手段

(5)を備えている請求項1～6何れか一記載の本人確認システム。

【請求項8】 プライベートデータは登録者の財産情報を含み、この財産情報の記録に基づいてサービス利用の適否を峻別する峻別出力を発する第2結果出力手段

(6)を備えている請求項7記載の本人確認システム。

【請求項9】 第2結果出力手段(6)は、財産情報が不良の場合、サービスの利用拒絶出力を発する財産不良者利用拒絶手段(61)である請求項8記載の本人確認システム。

【請求項10】 第2結果出力手段(6)は、財産情報

2

をサービスの利用側に通知する財産情報通知手段(62)である請求項8記載の本人確認システム。

【請求項11】 身体的個人情報は人の眼球情報である請求項1～10何れか一記載の本人確認システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、クレジットカードや電子マネーの利用等そのサービスを利用する際に会員資格等の一定の資格が求められる場合に、資格者本人たることを確認して第三者の不正な利用を効果的にカットできる本人確認システムに関する。

## 【0002】

【従来の技術】従来、クレジットカードの利用者は、自己のカードを加盟店等に提示してサイン等をすることにより一定限度内の買物をしたり、融資を受けたりできるようになっている。

## 【0003】

【発明が解決しようとする課題】しかし、カードが真正なら、たとえ本人でなくとも利用できてしまう問題があり、紛失・盗難等によりカードを無断使用された会員が損害を被る問題がある。又、カードが偽造され、カードチップをクリアしてしまえば、不法者の利用をそのまま許してしまう問題もあり、架空名義のカードによりクレジットカード会社等が損害を被る問題もある。

【0004】これらの防止策として、入会時、更新時等にカードに本人の顔写真を入れる提案があるが、写真を撮られたり、常時カードに自分の写真が付帯することについて抵抗感を覚える人が少なくないし、又、写真入りだと逆に持ち主がすぐに誰だかわかつて、その者をねらい打ちにした悪用を助長する懸念もある。

【0005】又、クレジットカードとは別に、指紋情報をデジタル化して本人確認用LSIカードに記録し、サービスの利用時にこのLSIカードと本人の指とを照合する提案もされている。しかしながら、カードを常時2枚携帯して運用する煩雑さがあるし、仮にクレジットカードとLSIカードとを1本化したとしても、常時ユーザーの末端において外部と接するカード自体に個人情報を付帯させているという点で、偽造の懸念が払拭できず、偽造団とのいたちごっこは不可避的であって、セキュリティを保証し難い致命的欠点がある。

【0006】本発明の主目的は、高いセキュリティの下で、真にサービスを利用し得る資格者本人たることを確認でき、第三者の不正利用による財産上の損失等を未然に防止できる本人確認システムを提供する点にある。

## 【0007】

【課題を解決するための手段】請求項1記載の発明は、上記主目的を達成するため、図1～7に示すように、資格者本人にサービスを提供する提供側Sとこのサービスを利用する利用側Rとの間に介在して、サービス利用者が資格者本人であるか否かを確認する本人確認システム

であつて、人の身体的個人情報 P a t A, P a t B . . . を識別子 I D A, I D B . . . と共に管理ファイル F 上に登録する個人情報登録手段 1、資格者たることを申告してサービスを利用する者が入力する身体的個人情報と既登録個人情報を照合する照合手段 2、入力した利用者の身体的個人情報と申告にかかる資格者の既登録個人情報が一致して資格者本人を確認する場合とこれ以外の場合とを峻別する峻別出力を発する結果出力手段 3 を備えている構成にした。

【0008】ここに、身体的個人情報は、人の目の眼球壁の最内層たる網膜の血管パターン（網膜パターン）や、虹彩の模様等の眼球情報の他、指紋等の個人によつて異なる全ての固有情報を含む概念である。識別子 I D A, I D B . . . は、多数登録する身体的個人情報 P a t A, P a t B . . . を相互に峻別するためのものであり、数桁の数字、文字、記号、これらの組合せ等から成り、パスワード、暗証番号、ID番号、氏名、生年月日、一般的の加入電話番号、携帯電話番号、クレジットカード番号等を含む概念である。サービスの利用時になされる資格者たることの申告は、クレジットカードの提示や、これに引き続くカードの読み取り、或は、キーボード K B 又は T K からのパスワードの手入力、申込書類への必要事項の記入、会員番号や氏名等の口答申告といった行為を含む概念である。

【0009】請求項 2 記載の発明は、本人確認のできない者のサービス利用を一層明確に排除するため、図 1, 2, 4, 5 に示すように、結果出力手段 3 は、資格者本人を確認できない場合、サービスの利用拒絶出力を発する確認不備者利用拒絶手段 3 1 であるものとした。この拒絶手段 3 1 は、図示のように、サービスの提供側 S、利用側 R、両者を結ぶ回線 L を含む情報伝達経路において、通常なら利用側 R と提供側 S とでやり取りされる取引き上のアクセス信号を自動的に断つたり受けないものとしたりする他、前記情報伝達経路の何れかの部分（例えば利用側 R）に設置するプリンター P 又は P r 、ディスプレイ D、ランプ E、ブザー等の出力手段に利用拒絶信号を出力させるものとしてもよい。

【0010】請求項 3 記載の発明は、サービス利用側 R の加盟店等で利用適格の有無をある程度判断することを要するが、システム構成を簡易にするため、図 3, 6, 7 に示すように、識別子 I D A, I D B . . . は、資格者たることを申告するサービス利用時に認識可能な情報であり、結果出力手段 3 は、入力した利用者の身体的個人情報と一致する既登録個人情報に付された識別子をサービスの利用側 R に通知する識別子通知手段 3 2 であるものとした。識別子 I D A, I D B . . . は、クレジットカード C D の固有情報では必ずしも無いもの（但しカード情報にも使われるものも含む）、例えば ID 番号、氏名、生年月日、一般的の加入電話番号や携帯電話番号等であつてもよいし、カード情報であるにしても、カード

番号や氏名等の表面記録情報（同時に内部記録情報でもあるものを含む）の他、専らカードリーダー C R 等で認識される内部記録情報も含む概念である。もっとも、運用の確実性からはカード情報、加盟店等での判断の迅速性を図る点からはそのうち特に表面記録情報とするのが好ましい。

【0011】請求項 4 記載の発明は、サービス利用時に利用者の既登録個人情報の検索時間を短縮して利用時の効率を高めるため、図 2, 3, 5, 6, 7 に示すよう

10 に、サービスの利用時に身体的個人情報と併用して入力する識別子 I D A, I D B . . . により、照合する既登録個人情報 P a t A, P a t B . . . を検索する検索手段 4 を備えている構成にした。識別子 I D A, I D B . . . は、その入力が利用者本人によりなされて秘密が保たれるのであれば、カード C D の暗証番号等の秘密情報であつてもよい。

【0012】請求項 5 記載の発明は、サービス利用側 R で利用適格の有無の判断がされる請求項 3 記載の発明において、サービス利用時の効率を極力高めると共に、識

20 別子の入力ミスをカバーし、正規利用者の利便を高めるため、図 3, 6, 7 に示すように、サービスの利用時に身体的個人情報と併用して入力する識別子 I D A, I D B . . . により、照合する既登録個人情報 P a t A, P a t B . . . を検索する検索手段 4、検索した既登録個人情報と入力した個人情報とが不一致の場合、入力した個人情報と他の既登録個人情報を照合するリカバリー手段 4 0 を備えている構成にした。

【0013】請求項 6 記載の発明は、個人情報の登録時やサービス利用時における処理効率を高めるため、図 1

30 ～ 6 に示すように、識別子 I D A, I D B . . . は、サービスの利用資格証であるカード C D に記録されたカード情報から成るものとした。カード情報は、表面記録情報、内部記録情報何れでもよいが、機械読み取りを容易にして処理効率向上の実効を図るために、内部記録情報（同時に表面記録情報であるものを含む）を用いるのが好ましい。

【0014】請求項 7 記載の発明は、本人確認だけでなく、多様なサービスの提供を可能にするため、図 4 ～ 7 に示すように、身体的個人情報 P a t A, P a t B . . . の登録者に対応するプライベートデータ P D A, P D B . . . にアクセスするデータアクセス手段 5 を備えている構成にした。プライベートデータ P D A, P D B . . . は、氏名、生年月日、性別、住所、電話番号、職業、財産情報等を広範囲に含み、識別子としても使えるもの（氏名等）をも包含する。

【0015】請求項 8 記載の発明は、資格者本人であつたとしても、財産情報の不良な者に対しては実際のサービスの利用は許可しないようにするため、同図 4 ～ 7 に示すように、プライベートデータ P D A, P D B . . . は登録者の財産情報 M D A, M D B . . . を含み、この

財産情報MDA, MDB・・・の記録に基づいてサービス利用の適否を峻別する峻別出力を発する第2結果出力手段6を備えている構成にした。財産情報MDA, MDB・・・は、カードCDの有効期限、融資限度、預金口座・残高、破産の有無（いわゆるブラックリスト）等を含み、その者の支払い能力を評価するあらゆる情報を包含する。

【0016】請求項9記載の発明は、財産情報不良者の明確な排除を図るために、図4, 5に示すように、第2結果出力手段6は、財産情報が不良の場合、サービスの利用拒絶出力を発する財産不良者利用拒絶手段61であるものとした。この財産不良者利用拒絶手段61も、上述した確認不備者利用拒絶手段31と同様、図示のように、サービスの提供側S、利用側R、両者を結ぶ回線Lを含む情報伝達経路中において、通常なら利用側Rと提供側Sとでやり取りされる取引き上のアクセス信号を自動的に断つたり受け付けないものとしたりする他、情報伝達経路の何れかの部分（例えば利用側R）に設置するプリンターピー又はPリ、ディスプレイD、ランプE、ブザー等の出力手段に利用拒絶信号を出力させるものとしてもよい。

【0017】請求項10記載の発明は、サービス利用側Rの加盟店等で財産不良者か否かをある程度判断することを要するが、システムの構成を簡易にするため、図6, 7に示すように、第2結果出力手段6は、財産情報をサービスの利用側Rに通知する財産情報通知手段62であるものとした。ここで通知する財産情報は、加盟店等での判断を容易化するため、融資限度や破産の有無といった明瞭なものであるのが好ましい。

【0018】請求項11記載の発明は、身体的個人情報の登録及び照合に際する信頼性及び精度の向上を図ると共に、指紋等と異なり、人に与える心理的抵抗感を少なくするため、図1～7に示すように、身体的個人情報は人の眼球情報であるものとした。眼球情報は、例えば網膜パターンならば、網膜パターン読取機10, 20の各ファインダー11, 21を覗き込む目から、赤外線等を使ってそのパターンが読み込まれるものである。

【0019】

【発明の作用効果】請求項1記載の発明では、図1～7に示すように、サービスを利用しようとする者は、先ず個人情報登録手段1により、各人の身体的個人情報（PatA等）を管理ファイルF上に登録する。多数登録する身体的個人情報PatA, PatB・・・は、識別子IDA, IDB・・・により相互に峻別される。

【0020】各加盟店等でサービスを利用する場合は、照合手段2により、その利用時に入力した個人情報と既登録個人情報とが照合される。照合によって一致する既登録個人情報が無い場合（会員だと言ってきたが、その利用者は実は会員ではなかった場合等）、並びに、入力した個人情報と一致する既登録個人情報は存在するが、

これと申告にかかる資格者の既登録個人情報が異なる場合（会員のAだと言ってきたが、その利用者は実は別の会員のBであった場合等）いずれも、結果出力手段3により、入力した個人情報と申告にかかる資格者の既登録個人情報が一致して資格者本人を確認する正規の場合（会員のAだと言ってきた利用者は本当にAだった場合）とは峻別されることになる。

【0021】これにより、資格者本人たることの確認された者のみが正規にサービスを利用でき、非会員等の未登録者及び会員であっても他人の資格を自己のものと偽る不正者等の利用は排除される。このシステムにおいて、各人の身体的個人情報PatA, PatB・・・は末端に開放されることなく管理ファイルF上でいわば内部管理されることになるため、偽造等の心配はなく、高いセキュリティを確保することができる。

【0022】請求項2記載の発明では、図1, 2, 4, 5に示すように、資格者本人を確認できない場合、確認不備者利用拒絶手段31から直接的にサービスの利用を拒絶する利用拒絶出力が発せられるため、不適格者の利用を一層明確に排除することができる。

【0023】請求項3記載の発明では、図3, 6, 7に示すように、入力した利用者の身体的個人情報と一致する既登録個人情報に付された識別子（IDA等）は、識別子通知手段32によりサービスの利用側Rに通知される。サービスの利用側Rでは、サービス利用に伴い認識できる識別子と通知のあった識別子との同一性を見極めることにより、サービス利用の適格者か否かを峻別できる。加盟店等で確認処理は幾分要するが、識別子IDAの通知のみでサービス利用の適否を峻別でき、システム構成を簡易にすることができる。

【0024】請求項4記載の発明では、図2, 3, 5, 6, 7に示すように、サービスの利用時、身体的個人情報と併用して識別子（IDA等）を入力することにより、多数ある既登録個人情報と逐一照合するのではなく、識別子に対応した既登録個人情報PatAを予め検索しておき、この既登録個人情報と入力した個人情報とを照合すれば足りるため、処理時間を短縮することができる。

【0025】請求項5記載の発明では、図3, 6, 7に示すように、検索手段4により、上記同様に処理時間を短縮することができる。一方、サービスの利用時に併用入力する識別子（例えばIDA）が読みミスや手入力ミス等により他のもの（例えばIDB）にシフトしていた場合、検索手段4で検索した既登録個人情報（PatB）と入力した個人情報（PatA）は不一致となる。しかしながら、引き続いて、リカバリー手段40により、入力した個人情報（PatA）と他の既登録個人情報（PatA, PatC・・・）とが照合され、当初から識別子による検索がない場合と同じ照合処理に自動的に移る。

【0026】そして、本来正規にサービスを利用し得る者は、他に該当する自己の既登録個人情報（Pat A）があり、これに対応した識別子（IDA）がサービスの利用側に通知される。この通知された識別子（IDA）は、併用入力した誤りの識別子（IDB）と異なるが、サービスの利用側では、カードの確認等により本来申告すべきであった正規の識別子（IDA）を確認できるため、サービス利用の適格者である旨の判断が行える。

【0027】尚、リカバリー手段40により通知された識別子（例えばIDC、従って利用者は実はC）が、利用者自身としては本来申告したかった識別子（IDA）と異なっていた場合は、勿論サービス利用の不適格者という判断となる（Aと偽ったが識別子をBと誤入力したC）。因に、この者が入力ミスせずにAの識別子（IDA）を入力したとしても、請求項1の説明で述べた通り、やはりサービス利用の不適格者という判断となる（会員のAを装った別会員C）。

【0028】請求項6記載の発明では図1～6に示すように、識別子IDA, IDB・・・はカードCDに記録されたカード情報であるため、別途に数桁の数字等を用意してキーボードKB又はTKから打ち込んだりする必要はなく、処理効率を高めることができると共に、利用者もその数桁の数字等を覚える必要もなく、運用を簡易にできる。

【0029】請求項7記載の発明では、図4～7に示すように、プライベートデータPDをデータアクセス手段5によりアクセスすることにより、登録者の利用状況の管理や登録者へのイベントの通知など多様なサービスの提供が可能になり、サービス性を向上することができる。

【0030】請求項8記載の発明では、同図4～7に示すように、資格者本人たることの確認ができた者であっても、財産情報MDA, MDB・・・の不良な者に対しては、第2結果出力手段6により実際のサービスの利用は排除できるため、一層適正な運用を担保することができる。

【0031】請求項9記載の発明では、図4, 5に示すように、財産情報が不良な場合、財産不良者利用拒絶手段61から直接的にサービスの利用を拒絶する利用拒絶出力が発せられるため、支払い不能等のトラブルを一層明確に排除することができる。

【0032】請求項10記載の発明では、図6, 7に示すように、財産情報（MDA等）は、財産情報通知手段62によりサービスの利用側Rに通知される。サービスの利用側Rでは、その通知のあった財産情報に基づいて支払い能力の有無を判断でき、資格者本人と確認される者であっても、この者に実際にサービスの利用を許してよいかどうかを岐別できる。加盟店等での確認処理は幾分要するが、財産情報MDAの通知だけでサービスの利用の適否を岐別でき、システム構成を簡易にすることが

できる。

【0033】請求項11記載の発明では、図1～7に示すように、身体的個人情報Pat A, Pat B・・・は人の眼球情報である。人間の網膜パターン等の眼球情報は人によって千差万別であり、しかも、指紋等と異なり、ファインダー11, 21から高品位なデータを取り込むことができる。このため、ミスが少なく、身体的個人情報の読み込みに際して信頼性及び精度を向上することができる。しかも、指紋等と異なり、登録及び照合時に心

10理的抵抗感を与えることもほとんどない。すなわち、指紋等は、その付着痕跡が犯罪検査に使われる事情から、伝統的に採取されるのに抵抗感を覚えるが、網膜パターン等の眼球情報ならば、それがどこかに付着するといったことは皆無であるため、犯罪検査の証拠となり得ず、逆に、登録事項とすることに抵抗感はほとんど生じない。

【0034】

【発明の実施の形態】図1において、Hは本人確認システムの中核を担う本人確認会社等の本人確認機関（以

20下、確認会社Hという）、Sはクレジットカード会社等のサービス提供機関（以下、クレジット会社Sとい）う）、Rは加盟店等の複数あるサービス利用機関（以下、加盟店Rとい）う）、Bはカード会員の登録を受ける銀行等の複数ある登録機関（以下、銀行Bとい）である。確認会社Hに設けるホストコンピュータHCと、クレジット会社S、加盟店R及び銀行Bの各コンピュータSC, RC, BCとは、通信回線Lを介して接続している。

【0035】銀行Bには、身体的個人情報たる網膜パタ

30ーンPat A, Pat B・・・を読取る網膜パターン読取機10を設置している。その登録は、入会者がファインダー11を左右何れかの片目で覗きながら登録キー12を押すことにより起動される。そして、確認会社Hにおいて、網膜パターン読取機10と連携するソフトウェア資源から成る個人情報登録手段1により、ホストコンピュータHCの管理ファイルF上に、その読取った網膜パターンのデジタル情報が識別子IDA, IDB・・・と共に登録される。

【0036】識別子IDA, IDB・・・は、カードC

40Dに記録されるカード番号等のカード情報から成り、その番号をコントロールパネル14から入力するようにしている。尚、銀行Bでカードが即日発効される場合やカードの更新登録時等には、その即日発効されるカードや旧カードをカードリーダーCRに通すことにより、自動的に識別子を入力できる。

【0037】ところで、銀行Bの網膜パターン読取機10は登録だけでなく、既登録パターンとの照合も行えるようになっており、ファインダー11を片目で覗きながら照合キー13を押すことにより、該当する既登録パタ

50ーンを抽出して、フロントディスプレイ15に該当登録

者の識別子（I D A等）と照合率を表示できるようになっている。

【0038】照合率は、覗き込む目の角度、姿勢等によって照合のたびに変動するが、最も近似した既登録パターンとの照合率が一定の基準値（例えば70%）以上の場合、同一であると判定し、この最近似パターンの識別子を照合率と共に表示するようにしているのである。基準値以上の照合率が得られない場合、該当登録が無い旨のコメントがフロントディスプレイ15に表示される。

【0039】加盟店Rには、ハンディリーダー200式の網膜パターン読取機20を設置している。店員は利用者から提示のあったカードCDをカードリーダーCRから読み込ませて資格者たることの申告をさせると共に、利用者にファインダー21を覗いてもらい、照合スイッチ22を押してもらう。これにより、確認会社Hにおいて、網膜パターン読取機20と連携するソフトウェア資源から成る照合手段2により、入力された網膜パターンと既登録パターンとが逐一照合されて、照合率が基準値（70%）以上の最も近似した該当パターンが選び出され、このパターンに対応した識別子（I DB等）が抽出される。

【0040】尚、照合率の基準値を如何に定めるかは、結局、誤認率をどの程度許容するかによる。因に70%であれば、数10万回～100万回に1回程度の誤認率に収まり、実使用上問題はない。もっとも、この数値よりも高い値、低い値を選定しても勿論よい。

【0041】こうして、以上の照合により、照合率が基準値以上の該当パターンがない場合（非会員の場合等）、並びに、該当パターンはあっても、これに対応した識別子（I DB）とカードCDから読み込んだ識別子（例えばI DA）とが異なる場合（不正会員Bが別会員Aの真正カードを無断使用した場合や別会員Aのカードを模した偽造カードを使用した場合等）、確認会社Hのソフトウェア資源たる結果出力手段3を構成する確認不備者利用拒絶手段31により、加盟店Rとクレジット会社Sとの間で通常やり取りされる取引上のアクセス信号を断ち、不正利用を自動的に排除するようになっている。又、同時に、通信回線Lを介して、加盟店R及びクレジット会社Sに利用を拒絶した旨を通知し、ディスプレイD、プリントP又はPr、ランプE等に表示させるよう正在している。

【0042】図2は第2実施形態を示し、このものは、サービスの利用時にカードリーダーCRから取り込まれる識別子I DA、I DB・・・により利用者の既登録パターンを予め検索しておく検索手段4を備え、検索したパターンと入力したパターンとが基準値以上の照合率となるか否かを調べ、照合処理時間を短縮できるようにしたものである。

【0043】非会員や不正会員が、他人の真正なカード

を無断使用したり別会員のカードを模した偽造カードを不正使用した場合は、入力したパターンと、他人のカード情報たる識別子に基づいて検索したパターンとは一致せず、照合率は基準値を下回り、上記同様に、確認不備者利用拒絶手段31により、これらの者の不正使用は排除される。

【0044】尚、図2のものでは、加盟店Rの網膜パターン読取機20を、銀行Bに設けた網膜パターン読取機10と同じ型式のものを用いているが、図1と同じくハンディリーダー式のものとしてもよい。又、図1において、加盟店Rの網膜パターン読取機20を銀行Bのものと同じ型式のものとしてもよいし、図1、2において、銀行Bの読取機10を、ハンディリーダー式のものとしてもよい。以下、図3以降のものも同様である。

【0045】図3は第3実施形態を示し、このものは、結果出力手段3を識別子通知手段31としたものであり、サービス利用時に入力したパターンと一致する既登録パターンに付された識別子（例えばI DA）を加盟店Rに通知して、そのディスプレイDやプリントP又はPrに出力させるよう正在している。

【0046】又、識別子による検索手段4の他に、検索した既登録パターンと入力したパターンとが不一致の場合、入力パターンと他の既登録パターンとを照合するリカバリー手段40を設け、通常は検索手段4により処理時間を見短縮する一方で、識別子の入力ミスのあるときに、リカバリー手段40によりそのミスをカバーし、正規利用者の利便を高め得るように正在している。

【0047】ところで、以上図1～3に示したものでは、確認会社Hではサービス利用者が資格者本人たるとの確認のみをするものとし、いわゆるブラックリストに載っているか否かは判断しないで、このような財産上の不良な会員の排除は、クレジット会社Sに委ねる仕様にしている。確認会社Hによる独自のサービスは本人確認のみに止まるが、個人のプライベートデータの管理を現状通りクレジット会社Sにそのまま集中保持させておくことができるメリットがある。

【0048】図4～6の第4～第6実施形態は、各々図1～3に対応（図4と図1、図5と図2、図6と図3）した基本仕様をもつが、更に、確認会社Hでイベントの通知や財産不良者の排除等を行えるようにしたのである。すなわち、確認会社Hの管理ファイルFに、登録者毎にプライベートデータPDA、PDB・・・の記憶領域を設け、これに氏名、生年月日、性別、住所、電話番号、職業等と共に、カードの有効期限、融資限度、預金口座・残高、破産の有無等の財産情報MDA、MDB・・・を記録している。そして、確認会社Hのソフトウェア資源であるデータアクセス手段5により、これらにアクセスし、メールの発送等を可能にしている共に、同第2結果出力手段6により、本人確認後の第2段階の処理として、財産情報の記録に基づく支払い能力の観点か

11

ら、サービスを実際に提供して差し支えの無い者か否かを峻別するようにしている。

【0049】図4、5のものは、第2結果出力手段6を財産不良者利用拒絶手段61としたものであり、カードの有効期限切れ、融資限度超え、残高不足、破産者の何れかに該当する財産情報不良者である場合、クレジット会社S、加盟店R、両者を結ぶ回線Lを含む情報伝達経路中に既述の確認不備者利用拒絶手段31と同様、サービスの利用拒絶出力を発して、通常やり取りされる取引き上のアクセス信号を断つようにしている。

【0050】又、図6のものは、第2結果出力手段6を財産情報通知手段62としたものであり、識別子の通知と共に、この識別子の通知がなされた者（資格者本人と確認されるべき者は勿論、確認されるべきでない者も含む）の財産情報、特にそのうち、良・不良を容易に判断できるカード有効期限、融資限度、破産の有無を加盟店Rに通知し、加盟店RのディスプレイDや、プリンタP又はPrに表示させるようにしている。

【0051】図7は第7実施形態を示し、このものは、網膜パターンの登録時にクレジットカードCDから識別子を読み込ませるといったカードとの併用運用を必要としない簡易なシステムであり、クレジットカードCDの存在と切り離して、個人情報たる網膜パターンの登録を可能にしたものである。

【0052】銀行B並びに加盟店Rの各網膜パターン読取機10、20のコントロールパネル14から識別子（例えば5桁のID番号と氏名及び生年月日）を入力すると共に、ファインダー11から網膜パターンPatA、PatB・・・を読み込ませて管理ファイルF上に登録できるようにしている。

【0053】そして、加盟店Rでの利用時には、網膜パターン読取機20からアクセスする照合を経てフロントディスプレイ15やプリンタPに出力される識別子（例えば氏名）と、持ち込まれたカードCDの表示や利用申

12

請用紙の表記とを目視確認することにより、本人確認できるようにしている。又、同時に通知される財産情報により、破産者か否かを判定できるようにしている。

【0054】尚、図1～7で、銀行Bの網膜パターン読取機10はクレジット会社Sに設置し、クレジット会社S自体で会員登録できるものとしても勿論よい。又、銀行Bや加盟店Rの網膜パターン読取機10、20は、それぞれの機関に具備するコンピュータBC、RCを介さずに、ダイレクトにホストコンピュータHCに接続する

- 10 ようにしてもよい。更に、図4、5の第2結果出力手段6に財産情報通知手段62を採用してもよいし、図6、7の第2結果出力手段6に財産不良者利用拒絶手段61を採用してもよい。

【図面の簡単な説明】

【図1】本発明に係る本人確認システムの第1実施形態の構成図。

【図2】同第2実施形態の構成図。

【図3】同第3実施形態の構成図。

【図4】同第4実施形態の構成図。

- 20 【図5】同第5実施形態の構成図。

【図6】同第6実施形態の構成図。

【図7】同第7実施形態の構成図。

【符号の説明】

1；個人情報登録手段

2；照合手段

3；結果出力手段

31；確認不備者利用拒絶手段

32；識別子通知手段

4；検索手段

- 30 40；リカバリー手段

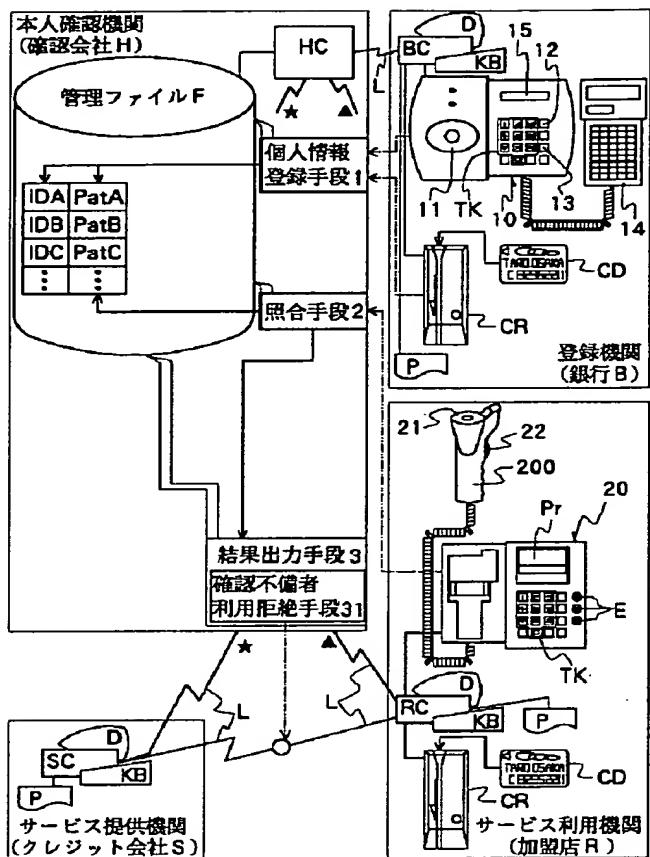
5；データアクセス手段

6；第2結果出力手段

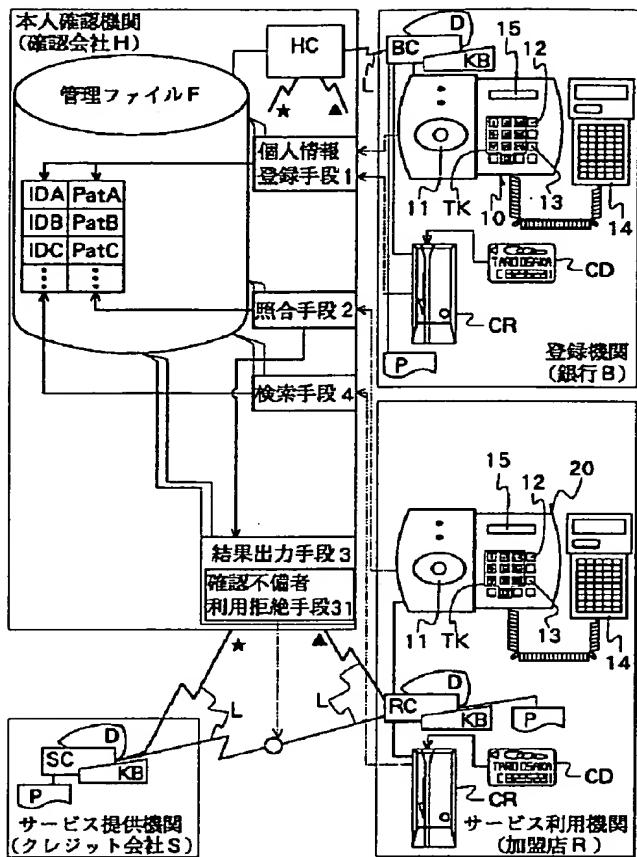
61；財産不良者利用拒絶手段

62；財産情報通知手段

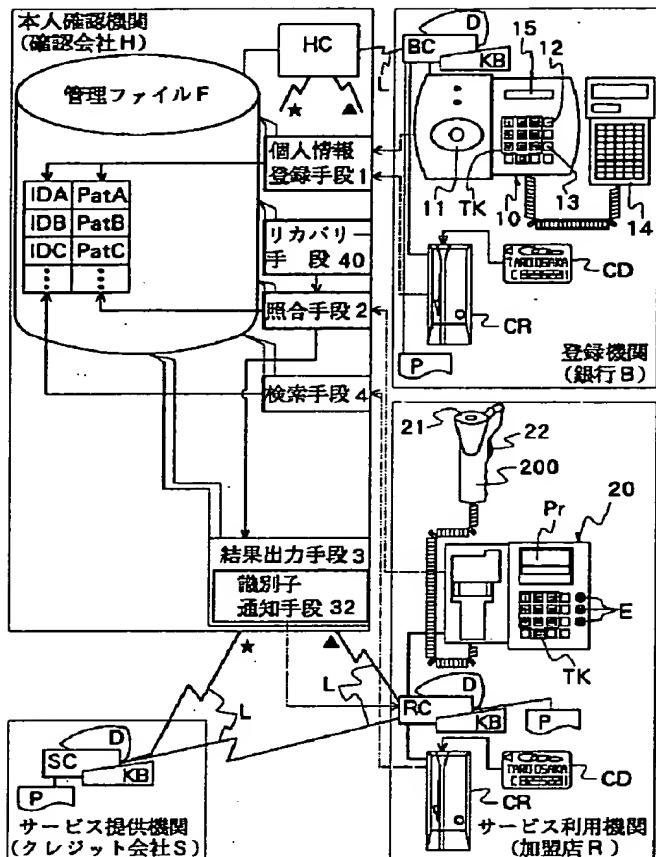
【図1】



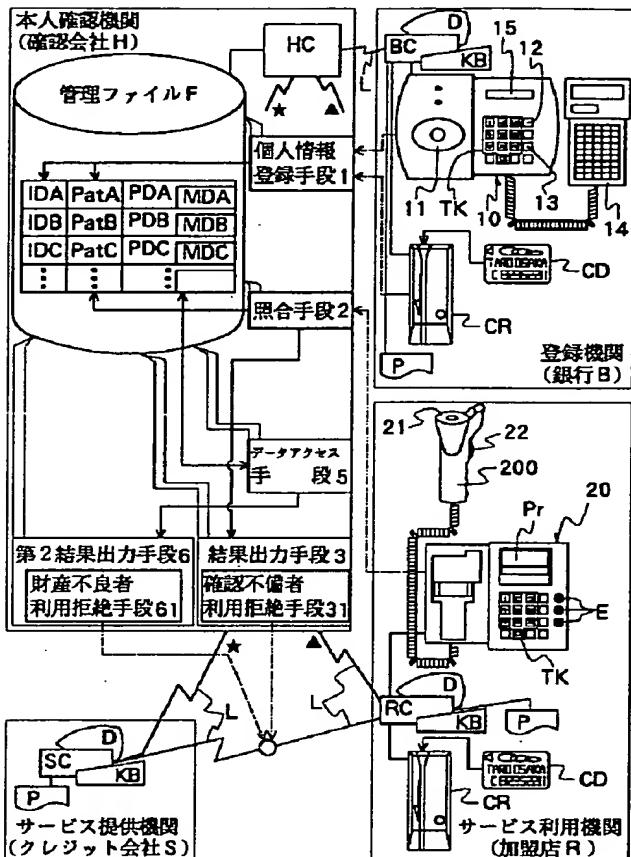
【図2】



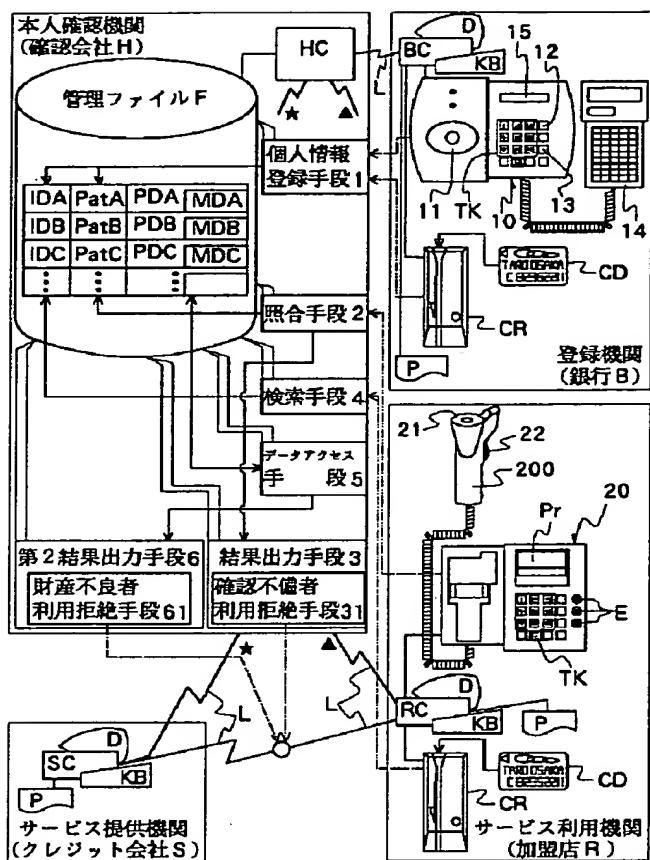
【図3】



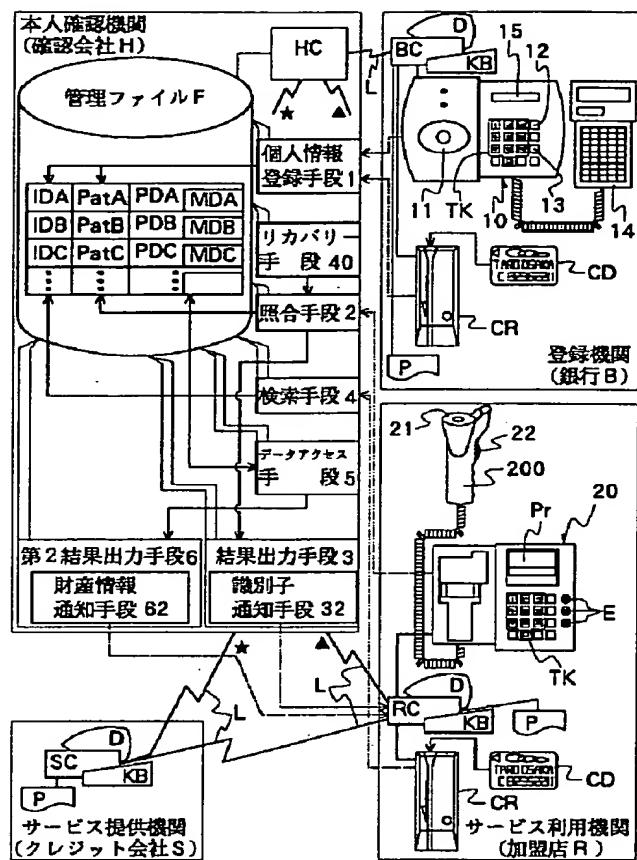
【図4】



【図5】



【図6】



【図7】

